

# National Cyber Alert System

[Archive](#)

## Cyber Security Bulletin SB09-229

### Vulnerability Summary for the Week of August 10, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities		
Primary Vendor -- Product	Description	Published
ooVoo	Buffer overflow in oovoo.exe in ooVoo 1.7.1.35, and possibly other versions before 1.7.1.59, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long oovoo: URI.	2009-08-12
aj_square -- aj_auction	AJ Square AJ Auction OOPD, Pro Platinum Skin #1, Pro Platinum Skin #2, and Web 2.0 send a redirect but do not exit when certain scripts are called directly, which allows remote attackers to bypass authentication via a direct request to (1) site.php, (2) auction.php, (3) mail.php, (4) fee_setting.php, (5) earnings.php, (6) insertion_fee_settings.php, (7) custom_category.php, (8) subcategory.php, (9) category.php, (10) report.php, (11) store_manager.php, and (12) choose_sell_format.php in admin/, and possibly other vectors.	2009-08-13
aj_square -- aj_auction	AJ Square AJ Auction Pro Platinum Skin #1 sends a redirect but does not exit when it is called directly, which allows remote attackers to bypass authentication via a direct request to admin/user.php.	2009-08-13
alstrasoft -- sendit	Unrestricted file upload vulnerability in submit_file.php in AlstraSoft SendIt Pro allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then	2009-08-11

	accessing it via a direct request to the file in send/files/.	
apache -- xerces-c++	Stack consumption vulnerability in validators/DTD/DTDScanner.cpp in Apache Xerces C++ 2.7.0 and 2.8.0 allows context-dependent attackers to cause a denial of service (application crash) via vectors involving nested parentheses and invalid byte values in "simply nested DTD structures," as demonstrated by the Codenomicon XML fuzzing framework.	2009-08-11
apple -- safari	Buffer overflow in WebKit in Apple Safari before 4.0.3 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted floating-point numbers.	2009-08-12
asterisk -- business_edition asterisk -- open_source asterisk -- opensource asterisk -- appliance_s800i	The SIP channel driver in Asterisk Open Source 1.2.x before 1.2.34, 1.4.x before 1.4.26.1, 1.6.0.x before 1.6.0.12, and 1.6.1.x before 1.6.1.4; Asterisk Business Edition A.x.x, B.x.x before B.2.5.9, C.x.x before C.2.4.1, and C.3.x before C.3.1; and Asterisk Appliance s800i 1.2.x before 1.3.0.3 does not use a maximum width when invoking sscanf style functions, which allows remote attackers to cause a denial of service (stack memory consumption) via SIP packets containing large sequences of ASCII decimal characters, as demonstrated via vectors related to (1) the CSeq value in a SIP header, (2) large Content-Length value, and (3) SDP.	2009-08-12
avira -- antivir avira -- antivir_personal avira -- antivir_professional avira -- antivir_security_suite	Avira AntiVir Premium, Premium Security Suite, AntiVir Professional, and AntiVir Personal - FREE allows local users to execute arbitrary code via a crafted IOCTL request that overwrites a kernel pointer.	2009-08-13
avira -- antivir avira -- antivir_security_suite	Unquoted Windows search path vulnerability in the scheduler (sched.exe) in Avira AntiVir, AntiVir Premium, Premium Security Suite, and AntiVir Professional might allow local users to gain privileges via a malicious antivir.exe file in the "C:\Program Files\avira\" directory.	2009-08-13
ca -- advantage_data_transport ca -- it_client_manager ca -- software_delivery ca -- unicenter_software_delivery	Stack-based buffer overflow in a token searching function in the dtscore library in Data Transport Services in CA Software Delivery r11.2 C1, C2, C3, and SP4; Unicenter Software Delivery 4.0 C3; CA Advantage Data Transport 3.0 C1; and CA IT Client Manager r12 allows remote attackers to execute arbitrary code via crafted data.	2009-08-10
chilkatsoft -- chilkat_socket	Insecure method vulnerability in the Chilkat Socket ActiveX control (ChilkatSocket.ChilkatSocket.1) in ChilkatSocket.dll 2.3.1.1 allows remote attackers to overwrite arbitrary files via the SaveLastError method. NOTE: this might be related to CVE-2008-1647.	2009-08-12
cms.maury91 -- maurycms	MauryCMS 0.53.2 and earlier does not require administrative authentication for Editors/fckeditor/editor/filemanager/browser/default/browser.html, which allows remote attackers to upload arbitrary files via a direct request.	2009-08-12
cms.maury91 -- maurycms	SQL injection vulnerability in Rss.php in MauryCMS 0.53.2 and earlier allows remote attackers to execute arbitrary SQL commands	2009-08-12

	via the c parameter.	12
collabtive -- collabtive	Collabtive 0.4.8 allows remote attackers to bypass authentication and create new users, including administrators, via unspecified vectors associated with the added mode in a users action to admin.php.	2009-08-12
cpanel -- cpanel	Directory traversal vulnerability in autoinstall4imagesgalleryupgrade.php in the Fantastico De Luxe Module for cPanel allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the scriptpath_show parameter in a GoAhead action. NOTE: the vendor and a third party suggest that this issue only crosses privilege boundaries when security settings such as disable_functions and safe_mode are active, since exploitation requires uploading of executable code to a home directory.	2009-08-10
curl -- libcurl libcurl -- libcurl	lib/ssluse.c in cURL and libcurl 7.4 through 7.19.5, when OpenSSL is used, does not properly handle a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-08-14
dd-wrt -- dd-wrt	httpd.c in httpd in the management GUI in DD-WRT 24 sp1 does not require administrative authentication for programs under cgi-bin/, which allows remote attackers to change settings via HTTP requests.	2009-08-14
discuz -- discuz!	member.php in Crossday Discuz! Board allows remote attackers to reset passwords of arbitrary users via crafted (1) lostpasswd and (2) getpasswd actions, possibly involving predictable generation of the id parameter.	2009-08-12
garagesalesjunkie -- garagesales_script	SQL injection vulnerability in visitor/view.php in GarageSales Script allows remote attackers to execute arbitrary SQL commands via the key parameter.	2009-08-14
gnu -- gnutls	libgnutls in GnuTLS before 2.8.2 does not properly handle a '\o' character in a domain name in the subject's (1) Common Name (CN) or (2) Subject Alternative Name (SAN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.	2009-08-12
	Stack-based buffer overflow in the _tt_internal_realpath function in	

ibm -- aix	the ToolTalk library (libtt.a) in IBM AIX 5.2.0, 5.3.0, 5.3.7 through 5.3.10, and 6.1.0 through 6.1.3, when the rpc.ttdbserver daemon is enabled in /etc/inetd.conf, allows remote attackers to execute arbitrary code via a long XDR-encoded ASCII string to remote procedure 15.	2009-08-10
ibm -- websphere_commerce	Multiple unspecified vulnerabilities in IBM WebSphere Commerce 6.0 before 6.0.0.7 have unknown impact and attack vectors.	2009-08-13
ibm -- websphere_application_server	The Security component in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.25 and 7.0 before 7.0.0.5 does not properly handle use of Identity Assertion with CSIV2 Security, which allows remote attackers to bypass intended CSIV2 access restrictions via vectors involving Enterprise JavaBeans (EJB).	2009-08-13
ibm -- websphere_application_server	The Servlet Engine/Web Container component in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.25 and 7.0 before 7.0.0.5, when SPNEGO Single Sign-on (SSO) and disableSecurityPreInvokeOnFilters are configured, allows remote attackers to bypass authentication via a request for a "secure URL," related to a certain invokefilterscompatibility property.	2009-08-13
ibm -- websphere_application_server	IBM WebSphere Application Server (WAS) 7.0 before 7.0.0.5 does not properly read the portletServingEnabled parameter in ibm-portlet-ext.xmi, which allows remote attackers to bypass intended access restrictions via unknown vectors.	2009-08-13
infireal -- mxcamarchive	mxCamArchive 2.2 stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain configuration details and passwords via a direct request for archive/config.ini.	2009-08-12
jabber -- exodus	Argument injection vulnerability in Exodus 0.10 allows remote attackers to inject arbitrary command line arguments, overwrite arbitrary files, and cause a denial of service via encoded spaces in a pres:// URI, a different vector than CVE-2008-6935.	2009-08-11
jabber -- exodus	Argument injection vulnerability in Exodus 0.10 allows remote attackers to inject arbitrary command line arguments, overwrite arbitrary files, and cause a denial of service via encoded spaces in an xmpp:// URI, a different vector than CVE-2008-6935 and CVE-2008-6936. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-08-11
joe_fuhrman -- exodus	Argument injection vulnerability in Exodus 0.10 allows remote attackers to inject arbitrary command line arguments, overwrite arbitrary files, and cause a denial of service via encoded spaces in an im:// URI.	2009-08-11
joomla -- com_content	SQL injection vulnerability in the content component (com_content) 1.0.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the Itemid parameter in a blogcategory action to index.php.	2009-08-10

memcachedb -- memcached	Multiple integer overflows in memcached 1.1.12 and 1.2.2 allow remote attackers to execute arbitrary code via vectors involving length attributes that trigger heap-based buffer overflows.	2009-08-10
michael_dehaan -- cobbler	The web interface (CobblerWeb) in Cobbler before 1.2.9 allows remote authenticated users to execute arbitrary Python code in cobbleld by editing a Cheetah kickstart template to import arbitrary Python modules.	2009-08-12
microsoft -- isa_server microsoft -- office microsoft -- office_web_components	The Office Web Components ActiveX Control in Microsoft Office XP SP3, Office 2003 SP3, Office XP Web Components SP3, Office 2003 Web Components SP3, Office 2003 Web Components SP1 for the 2007 Microsoft Office System, Internet Security and Acceleration (ISA) Server 2004 SP3 and 2006 SP1, and Office Small Business Accounting 2006 does not properly allocate memory, which allows remote attackers to execute arbitrary code via unspecified vectors that trigger "system state" corruption, aka "Office Web Components Memory Allocation Vulnerability."	2009-08-12
microsoft -- windows_2000 microsoft -- windows_server microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Heap-based buffer overflow in Microsoft Remote Desktop Connection (formerly Terminal Services Client) running RDP 5.0 through 6.1 on Windows, and Remote Desktop Connection Client for Mac 2.0, allows remote attackers to execute arbitrary code via unspecified parameters, aka "Remote Desktop Connection Heap Overflow Vulnerability."	2009-08-12
microsoft -- isa_server microsoft -- office microsoft -- office_web_components	Buffer overflow in the Office Web Components ActiveX Control in Microsoft Office XP SP3, Office 2000 Web Components SP3, Office XP Web Components SP3, BizTalk Server 2002, and Visual Studio .NET 2003 SP1 allows remote attackers to execute arbitrary code via crafted property values, aka "Office Web Components Buffer Overflow Vulnerability."	2009-08-12
microsoft -- windows_server microsoft -- windows_vista	ASP.NET in Microsoft .NET Framework 2.0 SP1 and SP2 and 3.5 Gold and SP1, when ASP 2.0 is used in integrated mode on IIS 7.0, does not properly manage request scheduling, which allows remote attackers to cause a denial of service (daemon outage) via a series of crafted HTTP requests, aka "Remote Unauthenticated Denial of Service in ASP.NET Vulnerability."	2009-08-12
microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Double free vulnerability in the Workstation service in Microsoft Windows allows remote authenticated users to gain privileges via a crafted RPC message to a Windows XP SP2 or SP3 or Server 2003 SP2 system, or cause a denial of service via a crafted RPC message to a Vista Gold, SP1, or SP2 or Server 2008 Gold or SP2 system, aka "Workstation Service Memory Corruption Vulnerability."	2009-08-12
microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Unspecified vulnerability in Avifil32.dll in the Windows Media file handling functionality in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via a malformed header in a crafted AVI file, aka "Malformed AVI Header Vulnerability."	2009-08-12
microsoft -- windows_2003_server microsoft -- windows_server_2008	Integer overflow in Avifil32.dll in the Windows Media file handling functionality in Microsoft Windows allows remote attackers to execute arbitrary code on a Windows 2000 SP4 system via a crafted	2009-08-12

microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	AVI file, or cause a denial of service on a Windows XP SP2 or SP3, Server 2003 SP2, Vista Gold, SP1, or SP2, or Server 2008 Gold or SP2 system via a crafted AVI file, aka "AVI Integer Overflow Vulnerability."	2009-08-12
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_vista microsoft -- windows_xp	The Message Queuing (aka MSMQ) service for Microsoft Windows 2000 SP4, XP SP2, Server 2003 SP2, and Vista Gold does not properly validate unspecified IOCTL request data from user mode before passing this data to kernel mode, which allows local users to gain privileges via a crafted request, aka "MSMQ Null Pointer Vulnerability."	2009-08-12
microsoft -- windows_2000 microsoft -- windows_2003_server	Heap-based buffer overflow in the Windows Internet Name Service (WINS) component for Microsoft Windows 2000 SP4 and Server 2003 SP2 allows remote attackers to execute arbitrary code via a crafted WINS replication packet that triggers an incorrect buffer-length calculation, aka "WINS Heap Overflow Vulnerability."	2009-08-12
microsoft -- windows_2000 microsoft -- windows_2003_server	Integer overflow in the Windows Internet Name Service (WINS) component for Microsoft Windows 2000 SP4 allows remote WINS replication partners to execute arbitrary code via crafted data structures in a packet, aka "WINS Integer Overflow Vulnerability."	2009-08-12
microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	Heap-based buffer overflow in the Microsoft Terminal Services Client ActiveX control running RDP 6.1 on Windows XP SP2, Vista SP1 or SP2, or Server 2008 Gold or SP2; or 5.2 or 6.1 on Windows XP SP3; allows remote attackers to execute arbitrary code via unspecified parameters to unknown methods, aka "Remote Desktop Connection ActiveX Control Heap Overflow Vulnerability."	2009-08-12
microsoft -- windows_2000 microsoft -- windows_2003_server microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	The Telnet service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote Telnet servers to execute arbitrary code on a client machine by replaying the NTLM credentials of a client user, aka "Telnet Credential Reflection Vulnerability," a related issue to CVE-2000-0834.	2009-08-12
microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp	The Active Template Library (ATL) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP2, Vista Gold, SP1, and SP2, and Server 2008 Gold and SP2 allows remote attackers to execute arbitrary code via vectors related to erroneous free operations after reading a variant from a stream and deleting this variant, aka "ATL Object Type Mismatch Vulnerability."	2009-08-12
microsoft -- biztalk_server microsoft -- internet_security_and_acceleration_server microsoft -- office microsoft -- office_web_components microsoft -- visual_studio_.net	Heap-based buffer overflow in the Office Web Components ActiveX Control in Microsoft Office XP SP3, Office 2003 SP3, Office XP Web Components SP3, Office 2003 Web Components SP3, Office 2003 Web Components SP1 for the 2007 Microsoft Office System, Internet Security and Acceleration (ISA) Server 2004 SP3 and 2006 SP1, and Office Small Business Accounting 2006 allows remote attackers to execute arbitrary code via unspecified parameters to unknown methods, aka "Office Web Components Heap Corruption Vulnerability."	2009-08-12
	The pf_test_rule function in OpenBSD Packet Filter (PF), as used in	

midnightbsd -- midnightbsd mirbsd -- miro netbsd -- netbsd openbsd -- openbsd	OpenBSD 4.2 through 4.5, NetBSD 5.0 before RC3, MirOS 10 and earlier, and MidnightBSD 0.3-current allows remote attackers to cause a denial of service (panic) via crafted IP packets that trigger a NULL pointer dereference during translation, related to an IPv4 packet with an ICMPv6 payload.	2009-08-11
pi3 -- pi3web	Pi3Web 2.0.3 before PL2, when installed on Windows as a desktop application and without using the Pi3Web/Conf/Intenet.pi3, allows remote attackers to cause a denial of service (crash or hang) and obtain the full pathname of the server via a request to a file in the ISAPI directory that is not an executable DLL, which triggers the crash when the DLL load fails, as demonstrated using Isapi\users.txt.	2009-08-11
pligg -- pligg_cms	Multiple SQL injection vulnerabilities in submit.php in Pligg CMS 9.9.5 allow remote attackers to execute arbitrary SQL commands via the (1) category and (2) id parameters.	2009-08-13
sansuart -- free_simple_guestbook_php_script	Static code injection vulnerability in Sanus artificium (aka Sanusart) Free simple guestbook PHP script, when downloaded before 20081111, allows remote attackers to inject arbitrary PHP code into messages.txt via the message parameter to act.php, which is executed when guestbook/guestbook.php is accessed. NOTE: some of these details are obtained from third party information.	2009-08-11
shop-o2o -- php_paid_4_mail_script	PHP remote file inclusion vulnerability in home.php in PHP Paid 4 Mail Script allows remote attackers to execute arbitrary PHP code via a URL in the page parameter.	2009-08-14
simplemachines -- smf	The password reset functionality in Simple Machines Forum (SMF) 1.0.x before 1.0.14, 1.1.x before 1.1.6, and 2.0 before 2.0 beta 4 includes clues about the random number generator state within a hidden form field and generates predictable validation codes, which allows remote attackers to modify passwords of other users and gain privileges.	2009-08-13
snom -- snom_voip_phone snom -- snom_320_linux	The web interface on the snom VoIP phones snom 300, snom 320, snom 360, snom 370, and snom 820 with firmware 6.5 before 6.5.20, 7.1 before 7.1.39, and 7.3 before 7.3.14 allows remote attackers to bypass authentication, and reconfigure the phone or make arbitrary use of the phone, via a (1) http or (2) https request with 127.0.0.1 in the Host header.	2009-08-14
subversion -- subversion	Multiple integer overflows in the libsvn_delta library in Subversion before 1.5.7, and 1.6.x before 1.6.4, allow remote authenticated users and remote Subversion servers to execute arbitrary code via an svndiff stream with large windows that trigger a heap-based buffer	2009-08-07

	overflow, a related issue to CVE-2009-2412.	
sun -- openjdk	The Java Web Start framework in IcedTea in OpenJDK before 1.6.0.0-20.b16.fc10 on Fedora 10, and before 1.6.0.0-27.b16.fc11 on Fedora 11, trusts an entire application when at least one of the listed jar files is trusted, which allows context-dependent attackers to execute arbitrary code without the untrusted-code restrictions via a crafted application, related to NetX.	2009-08-10
sun -- java_se sun -- openjdk	Sun Java SE 5.0 before Update 20 and 6 before Update 15, and OpenJDK, might allow context-dependent attackers to obtain sensitive information via vectors involving static variables that are declared without the final keyword, related to (1) LayoutQueue, (2) Cursor.predefined, (3) AccessibleResourceBundle.getContents, (4) ImageReaderSpi.STANDARD_INPUT_TYPE, (5) ImageWriterSpi.STANDARD_OUTPUT_TYPE, (6) the imageio plugins, (7) DnsContext.debug, (8) RmfFileReader/StandardMidiFileWriter.types, (9) AbstractSaslImpl.logger, (10) Synth.Region.uiToRegionMap/lowerCaseNameMap, (11) the Introspector class and a cache of BeanInfo, and (12) JAX-WS, a different vulnerability than CVE-2009-2673.	2009-08-10
sun -- java_se sun -- openjdk	The Java Management Extensions (JMX) implementation in Sun Java SE 6 before Update 15, and OpenJDK, does not properly enforce OpenType checks, which allows context-dependent attackers to bypass intended access restrictions by leveraging finalizer resurrection to obtain a reference to a privileged object.	2009-08-10
sun -- java_se sun -- openjdk	JDK13Services.getProviders in Sun Java SE 5.0 before Update 20 and 6 before Update 15, and OpenJDK, grants full privileges to instances of unspecified object types, which allows context-dependent attackers to bypass intended access restrictions via an untrusted (1) applet or (2) application.	2009-08-10
sun -- java_se	The plugin functionality in Sun Java SE 6 before Update 15 does not properly implement version selection, which allows context-dependent attackers to leverage vulnerabilities in "old zip and certificate handling" and have unspecified other impact via unknown vectors.	2009-08-10
sun -- java_se	Multiple unspecified vulnerabilities in the Provider class in Sun Java SE 5.0 before Update 20 have unknown impact and attack vectors, aka BugId 6406003.	2009-08-10
sun -- java_se	Multiple unspecified vulnerabilities in the Provider class in Sun Java SE 5.0 before Update 20 have unknown impact and attack vectors, aka BugId 6429594. NOTE: this issue exists because of an incorrect fix for BugId 6406003.	2009-08-10
sun -- java_se	Unspecified vulnerability in deserialization in the Provider class in Sun Java SE 5.0 before Update 20 has unknown impact and attack vectors, aka BugId 6444262.	2009-08-10

sun -- java_se	Race condition in the java.lang package in Sun Java SE 5.0 before Update 20 has unknown impact and attack vectors, related to a "3Y Race condition in reflection checks."	2009-08-10
turnkeyforms -- web_hosting_directory	TurnkeyForms Web Hosting Directory allows remote attackers to bypass authentication and (1) gain administrative privileges by setting the adm cookie to 1 or (2) gain privileges as another user by setting the logged cookie to the target username.	2009-08-12
turnkeyforms -- web_hosting_directory	TurnkeyForms Web Hosting Directory stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain a database backup via a direct request to admin/backup/db.	2009-08-12
turnkeyforms -- web_hosting_directory	SQL injection vulnerability in the login functionality in TurnkeyForms Web Hosting Directory allows remote attackers to execute arbitrary SQL commands via the password field.	2009-08-12
turnkeyforms -- text_link_sales	admin.php in TurnkeyForms Text Link Sales allows remote attackers to bypass authentication and gain administrative privileges via a direct request.	2009-08-13
ubbcentral -- ubb.threads	SQL injection vulnerability in dosearch.inc.php in UBB.threads 7.3.1 and earlier allows remote attackers to execute arbitrary SQL commands via the Forum[] array parameter.	2009-08-13
webhost-panel -- bankoi_webhosting_control_panel	Multiple SQL injection vulnerabilities in login.asp in Bankoi WebHosting Control Panel 1.20 allow remote attackers to execute arbitrary SQL commands via the (1) username or (2) password field.	2009-08-12
wordpress -- wordpress	wp-login.php in WordPress 2.8.3 and earlier allows remote attackers to force a password reset for the first user in the database, possibly the administrator, via a key[] array variable in a resetpass (aka rp) action, which bypasses a check that assumes that \$key is not an array.	2009-08-13
x7_group -- x7_chat	SQL injection vulnerability in the login page in X7 Chat 2.0.5 allows remote attackers to execute arbitrary SQL commands via the password field.	2009-08-13
	Multiple stack-based buffer overflows in CMailCOM.dll in CMailServer 5.4.6 allow remote attackers to execute arbitrary code via a long argument to the (1) CreateUserPath, (2) Logout, (3) DeleteMailByUID, (4) MoveToInbox, (5) MoveToFolder, (6) DeleteMailEx, (7) GetMailDataEx, (8) SetReplySign, (9)	

youngzsoft -- emailserver	SetForwardSign, and (10) SetReadSign methods, which are not properly handled by (a) the POP3 Class ActiveX control (CMailCom.POP3); or a long argument to the (11) AddAttach, (12) SetSubject, (13) SetBcc, (14) SetBody, (15) SetCc, (16) SetFrom, (17) SetTo, and (18) SetFromUID methods, which are not properly handled by the Class ActiveX control (CMailCOM.SMTP), as demonstrated via the indexOfMail parameter to mwmail.asp.	2009-08-10
zeeways -- shaadiclone	Zeeways SHAADICLONE 2.0 allows remote attackers to bypass authentication and gain administrative privileges via a direct request to admin/home.php.	2009-08-07
zope -- zodb	Zope Object Database (ZODB) before 3.8.2, when certain Zope Enterprise Objects (ZEO) database sharing is enabled, allows remote attackers to bypass authentication via vectors involving the ZEO network protocol.	2009-08-07

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
alt-n -- mddaemon alt-n -- worldclient	Multiple unspecified vulnerabilities in WorldClient in Alt-N MDaemon before 10.02 have unknown impact and attack vectors, probably related to cross-site scripting (XSS) and WorldClient DLL 10.0.1, a different vulnerability than CVE-2008-6893.	2009-08-13	5.0	<a href="#">CVE-2008-6967 CONFIRM</a>
apple -- safari apple -- mac_os_x apple -- mac_os_x_server microsoft -- windows_vista microsoft -- windows_xp	Unspecified vulnerability in Apple Safari 4 before 4.0.3 allows remote web servers to place an arbitrary web site in the Top Sites view, and possibly conduct phishing attacks, via unknown vectors.	2009-08-12	5.0	<a href="#">CVE-2009-2196 SECTRACK BID CONFIRM APPLE</a>
apple -- safari	Incomplete blacklist vulnerability in WebKit in Apple Safari before 4.0.3 allows remote attackers to spoof domain names in URLs, and possibly conduct phishing attacks, via unspecified homoglyphs.	2009-08-12	4.3	<a href="#">CVE-2009-2199 CONFIRM APPLE</a>
apple -- safari	WebKit in Apple Safari before 4.0.3 does not properly restrict the URL scheme of the pluginspage attribute of an EMBED element, which allows user-assisted remote attackers to launch arbitrary file: URLs and obtain sensitive information via a crafted HTML document.	2009-08-12	4.3	<a href="#">CVE-2009-2200 CONFIRM APPLE</a>
ca -- siteminder sun -- j2ee	CA SiteMinder allows remote attackers to bypass cross-site scripting (XSS) protections for J2EE applications via a request containing a %00 (encoded null byte).	2009-08-11	4.3	<a href="#">CVE-2009-2704 MISC</a>
ca -- siteminder sun -- j2ee	CA SiteMinder allows remote attackers to bypass cross-site scripting (XSS) protections for J2EE applications via a request containing non-canonical, "overlong Unicode" in place of blacklisted characters.	2009-08-11	4.3	<a href="#">CVE-2009-2705 MISC</a>
collabtive -- collabtive	Cross-site scripting (XSS) vulnerability in manageproject.php in Collabtive 0.4.8 allows user-assisted remote attackers to inject arbitrary web script or HTML via the project Name, which is not properly handled when the administrator performs an editform	2009-08-12	4.3	<a href="#">CVE-2008-6946 XF BID BUGTRAQ</a>

	action, related to admin.php.		MILWORM
collabtive -- collabtive	Unrestricted file upload vulnerability in Collabtive 0.4.8 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension and using a text/plain MIME type, then accessing it via a direct request to the file in files/, related to (1) the showproject action in managefile.php or (2) the Messages feature.	2009-08-12	6.5 CVE-2008-6948 XF BID BUGTRAQ MILWORM
collabtive -- collabtive	Multiple cross-site request forgery (CSRF) vulnerabilities in Collabtive 0.4.8 allow remote attackers to hijack the authentication of administrators for requests that (1) submit or edit a new project, or (2) upload files to a project, or (3) attach files to messages via unknown vectors. NOTE: these issues can be leveraged with other vulnerabilities to create remote attack vectors that do not require authentication.	2009-08-12	6.8 CVE-2008-6949 BUGTRAQ MILWORM
comsenz -- crossday_discuz!_board	wap/index.php in Crossday Discuz! Board 6.x and 7.x allows remote authenticated users to execute arbitrary PHP code via the creditsformula parameter.	2009-08-12	6.5 CVE-2008-6958 XF BID MILWORM MISC MISC SECUNIA OSVDB
cpanel -- cpanel	Multiple cross-site scripting (XSS) vulnerabilities in autoinstall4imagesgalleryupgrade.php in the Fantastico De Luxe Module for cPanel allow remote attackers to inject arbitrary web script or HTML via the (1) localapp, (2) updatedir, (3) scriptpath_show, (4) domain_show, (5) thispage, (6) thisapp, and (7) currentversion parameters in an Upgrade action.	2009-08-10	4.3 CVE-2008-6927 XF BUGTRAQ BUGTRAQ BUGTRAQ OSVDB MISC MILWORM SECUNIA
dd-wrt -- dd-wrt	Multiple cross-site request forgery (CSRF) vulnerabilities in apply.cgi in DD-WRT 24 sp1 and earlier allow remote attackers to hijack the authentication of administrators for requests that (1) execute arbitrary commands via the ping_ip parameter; (2) change the administrative credentials via the http_username and http_passwd parameters; (3) enable remote administration via the remote_management parameter; or (4) configure port forwarding via certain from, to, ip, and pro parameters.	2009-08-14	6.8 CVE-2008-6974 BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ MILWORM MISC
dd-wrt -- dd-wrt	Multiple cross-site request forgery (CSRF) vulnerabilities in apply.cgi in DD-WRT 24 sp2 allow remote attackers to hijack the authentication of administrators for requests that (1) execute arbitrary commands via the ping_ip parameter; (2) change the administrative credentials via the http_username and http_passwd parameters; (3) enable remote administration via the remote_management parameter; or (4) configure port forwarding via certain from, to, ip, and pro parameters. NOTE: This issue reportedly exists because of a "weak ... anti-CSRF fix" implemented in 24 sp2.	2009-08-14	6.8 CVE-2008-6975 BUGTRAQ BUGTRAQ BUGTRAQ MILWORM MISC

fetchmail -- fetchmail	socket.c in fetchmail before 6.3.11 does not properly handle a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-08-07	6.4	CVE-2009-2666 VUPEN SLACKWARE SECTRACK BID BUGTRAQ MANDRIVA DEBIAN SECUNIA SECUNIA SECUNIA OSVDB MLIST CONFIRM
freearcadescript -- free_arena_script	Cross-site scripting (XSS) vulnerability in Free Arcade Script 1.3 allows remote attackers to inject arbitrary web script or HTML via the keyword parameter to the default URI under search/.	2009-08-14	4.3	CVE-2009-2771 SECUNIA MISC OSVDB
freenas -- freenas	Cross-site request forgery (CSRF) vulnerability in the WebGUI in FreeNAS before 0.7RC1 allows remote attackers to hijack the authentication of users for unspecified requests via unknown vectors.	2009-08-11	4.3	CVE-2009-2738 CONFIRM
freenas -- freenas	Cross-site scripting (XSS) vulnerability in FreeNAS before 0.69.2 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	2009-08-11	4.3	CVE-2009-2739 CONFIRM JVNDB JVN
garagesalesjunkie -- garagesales_script	Cross-site scripting (XSS) vulnerability in visitor/view.php in GarageSales Script allows remote attackers to inject arbitrary web script or HTML via the key parameter. NOTE: some of these details are obtained from third party information.	2009-08-14	4.3	CVE-2009-2778 XF VUPEN MILWORM SECUNIA
hp -- hpx	Unspecified vulnerability in HP-UX B.11.31 allows local users to cause a denial of service (system crash) via unknown vectors related to the ttrace system call.	2009-08-12	4.9	CVE-2009-1427 VUPEN SECTRACK
hp -- insight_control_suite_for_linux	Cross-site request forgery (CSRF) vulnerability in HP Insight Control Suite For Linux (aka ICE-LX) before 2.11 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.	2009-08-14	6.8	CVE-2009-2677 HP HP
ibm -- websphere_application_server	The Service Component Architecture (SCA) feature pack for IBM WebSphere Application Server (WAS) SCA 1.0 before 1.0.0.3 allows remote authenticated users to bypass intended authentication.transport access restrictions and obtain unspecified access via unknown vectors.	2009-08-13	6.5	CVE-2009-0906 XF
ibm -- websphere_application_server	Unspecified vulnerability in wsadmin in the System Management/Repository component in IBM WebSphere Application Server (WAS) 7.0 before 7.0.0.5 allows remote attackers to bypass intended Java Management Extensions (JMX) Management Beans (aka MBeans) access restrictions, and cause a denial of service (daemon stop), via unknown vectors.	2009-08-13	5.0	CVE-2009-2090 CONFIRM

ibm -- websphere_application_server	The System Management/Repository component in IBM WebSphere Application Server (WAS) 7.0 before 7.0.0.5 on z/OS uses weak file permissions for new applications, which allows remote attackers to obtain sensitive information via unspecified vectors.	2009-08-13	5.0	CVE-2009-2091 CONFIRM
ibm -- websphere_partner_gateway	SQL injection vulnerability in the console in IBM WebSphere Partner Gateway (WPG) Enterprise 6.0 before FP8, 6.1 before FP3, 6.1.1 before FP2, and 6.2 before FP1 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors.	2009-08-13	6.5	CVE-2009-2093 CONFIRM
icdevgroup -- interchange	Multiple cross-site scripting (XSS) vulnerabilities in Interchange 5.7 before 5.7.1, 5.6 before 5.6.1, and 5.4 before 5.4.3 allow remote attackers to inject arbitrary web script or HTML via (1) the mv_order_item CGI variable parameter in Core, (2) the country-select widget, or (3) possibly the value specifier when used in the UserTag feature.	2009-08-12	4.3	CVE-2008-6945 CONFIRM
infireal -- mxcamarchive	Static code injection vulnerability in admin/admin.php in mxCamArchive 2.2 allows remote authenticated administrators to inject arbitrary PHP code into an unspecified program via the description parameter, which is executed by invocation of index.php. NOTE: some of these details are obtained from third party information.	2009-08-12	6.5	CVE-2008-6956 XF MILWORM SECUNIA OSVDB
intelliants -- esyndicat	Multiple cross-site scripting (XSS) vulnerabilities in register.php in eSyndiCat Directory 2.2 allow remote attackers to inject arbitrary web script or HTML via the (1) username, (2) email, (3) password, (4) password2, (5) security_code, and (6) register parameters.	2009-08-10	4.3	CVE-2008-6924 XF BID OSVDB SECUNIA MISC
microsoft -- internet_explorer microsoft -- windows_7	Microsoft Internet Explorer 8.0.7100.0 on Windows 7 RC on the x64 platform allows remote attackers to cause a denial of service (application crash) via a certain DIV element in conjunction with SCRIPT elements that have empty contents and no reference to a valid external script location.	2009-08-14	5.0	CVE-2009-2764 BID MILWORM
minigal -- minigal	Directory traversal vulnerability in index.php in MiniGal b13 (aka MG2) allows remote attackers to read the source code of .php files, and possibly the content of other files, via a .. (dot dot) in the list parameter.	2009-08-11	5.0	CVE-2008-6933 XF BID MILWORM
mozilla -- seamonkey mozilla -- thunderbird	mailnews in Mozilla Thunderbird before 2.0.0.18 and SeaMonkey before 1.1.13, when JavaScript is enabled in mail, allows remote attackers to obtain sensitive information about the recipient, or comments in forwarded mail, via script that reads the (1) .documentURI or (2) .textContent DOM properties.	2009-08-13	4.3	CVE-2008-6961 CONFIRM XF SECTRACK BID CONFIRM SECUNIA SECUNIA
pentasoft_corp. -- avactis_shopping_cart	Multiple cross-site scripting (XSS) vulnerabilities in checkout.php in Avactis Shopping Cart 1.8.0 and 1.8.1 allow remote attackers to inject arbitrary web script or HTML via the (1) step_id and (2)	2009-08-13	4.3	CVE-2008-6969 XF BID CONFIRM SECUNIA

	CHECKOUT_CZ_BLOWFISH_KEY parameters.			<a href="#">SECUNIA</a> <a href="#">OSVDB</a> <a href="#">MISC</a>
phpstore -- complete_classifieds	Unrestricted file upload vulnerability in PHPStore Complete Classifieds allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension as a logo, then accessing it via a direct request to the file in classifieds1/yellow_images/.	2009-08-11	<a href="#">6.5</a>	<a href="#">CVE-2008-6928</a> <a href="#">VUPEN</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
phpstore -- auto_classifieds	Unrestricted file upload vulnerability in PHPStore Auto Classifieds allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension as a logo, then accessing it via a direct request to the file in cars/cars_images/.	2009-08-11	<a href="#">6.5</a>	<a href="#">CVE-2008-6929</a> <a href="#">VUPEN</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
phpstore -- real_estate	Unrestricted file upload vulnerability in PHPStore Real Estate allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension as a logo, then accessing it via a direct request to the file in realty/re_images/.	2009-08-11	<a href="#">6.5</a>	<a href="#">CVE-2008-6930</a> <a href="#">VUPEN</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
phpstore -- phpcareers	Unrestricted file upload vulnerability in PHPStore Job Search (aka PHPCareers) allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension as a resume photo, then accessing it via a direct request to the file in jobseekers/jobseeker_profile_images/.	2009-08-11	<a href="#">6.5</a>	<a href="#">CVE-2008-6931</a> <a href="#">VUPEN</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
realtysoft -- pg_roomate_finder_solution	Multiple cross-site scripting (XSS) vulnerabilities in PG Roommate Finder Solution allow remote attackers to inject arbitrary web script or HTML via the part parameter to (1) quick_search.php and (2) viewprofile.php.	2009-08-14	<a href="#">4.3</a>	<a href="#">CVE-2009-2772</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">MISC</a> <a href="#">OSVDB</a> <a href="#">OSVDB</a>
scriptsfeed -- realtor_classifieds_system	Unrestricted file upload vulnerability in ScriptsFeed Realtor Classifieds System (aka Real Estate Classifieds) allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension as a profile logo, then accessing it via a direct request to the file in re_images/.	2009-08-12	<a href="#">6.5</a>	<a href="#">CVE-2008-6942</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
scriptsfeed -- recipes_listing_portal	Unrestricted file upload vulnerability in ScriptsFeed Recipes Listing Portal allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension as a recipe photo, then accessing it via a direct request to the file in pictures/.	2009-08-12	<a href="#">6.5</a>	<a href="#">CVE-2008-6943</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
scriptsfeed -- auto_classifieds	Unrestricted file upload vulnerability in ScriptsFeed Auto Classifieds allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension as a profile logo, then accessing it via a direct request to the file in cars_images/.	2009-08-12	<a href="#">6.5</a>	<a href="#">CVE-2008-6944</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
	The CDCServlet component in Sun Java System Access			

sun -- java_system_access_manager sun -- java_system_web_server	Manager 7.0 2005Q4 and 7.1, when Cross Domain Single Sign On (CDSSO) is enabled, does not ensure that "policy advice" is presented to the correct client, which allows remote attackers to obtain sensitive information via unspecified vectors.	2009-08-07	4.3	CVE-2009-2713 BID CONFIRM
sun -- virtualbox	Unspecified vulnerability in Sun VirtualBox 3.0.0 and 3.0.2 allows guest OS users to cause a denial of service (host OS reboot) via unknown vectors.	2009-08-07	4.9	CVE-2009-2714 VUPEN BID SUNALERT SECUNIA
sun -- java_se sun -- openjdk	The encoder in Sun Java SE 6 before Update 15, and OpenJDK, grants read access to private variables with unspecified names, which allows context-dependent attackers to obtain sensitive information via an untrusted (1) applet or (2) application.	2009-08-10	5.0	CVE-2009-2690 CONFIRM
sun -- java_se	The Abstract Window Toolkit (AWT) implementation in Sun Java SE 6 before Update 15 on Windows 2000 Professional does not provide a Security Warning Icon, which makes it easier for context-dependent attackers to trick a user into interacting unsafely with an untrusted applet.	2009-08-10	6.8	CVE-2009-2717 CONFIRM
sun -- java_se	The Abstract Window Toolkit (AWT) implementation in Sun Java SE 6 before Update 15 on X11 does not impose the intended constraint on distance from the window border to the Security Warning Icon, which makes it easier for context-dependent attackers to trick a user into interacting unsafely with an untrusted applet.	2009-08-10	6.8	CVE-2009-2718 CONFIRM
sun -- java_se	The Java Web Start implementation in Sun Java SE 6 before Update 15 allows context-dependent attackers to cause a denial of service (NullPointerException) via a crafted .jnlp file, as demonstrated by the jnlp_file/appletDesc/index.html#misc test in the Technology Compatibility Kit (TCK) for the Java Network Launching Protocol (JNLP).	2009-08-10	5.0	CVE-2009-2719 CONFIRM
sun -- java_se	Unspecified vulnerability in the javax.swing.plaf.synth.SynthContext.isSubregion method in the Swing implementation in Sun Java SE 6 before Update 15 allows context-dependent attackers to cause a denial of service (NullPointerException in the Jemmy library) via unknown vectors.	2009-08-10	5.0	CVE-2009-2720 CONFIRM
sun-jester -- opennews	SQL injection vulnerability in admin.php in sun-jester OpenNews 1.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-08-11	6.8	CVE-2009-2735 XF VUPEN MILWORM SECUNIA OSVDB
sun-jester -- opennews	Static code injection vulnerability in admin.php in sun-jester OpenNews 1.0 allows remote authenticated administrators to inject arbitrary PHP code into config.php via the "Overall Width" field in a setconfig action.	2009-08-11	6.5	CVE-2009-2736 XF VUPEN MILWORM SECUNIA OSVDB
	The EditCSVAction function in cgi/actions.py in			

toni_mueller -- roundup	Roundup 1.2 before 1.2.1, 1.4 through 1.4.6, and possibly other versions does not properly check permissions, which allows remote authenticated users with edit or create privileges for a class to modify arbitrary items within that class, as demonstrated by editing all queries, modifying settings, and adding roles to users.	2009-08-11	5.5	CVE-2009-2737 DEBIAN
ultrize -- timesheet	PHP remote file inclusion vulnerability in include/timesheet.php in Ultrize TimeSheet 1.2.2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the config[include_dir] parameter.	2009-08-14	6.8	CVE-2009-2769 MILWORM SECUNIA
x10media -- .x10_automatic_mp3_script	download.php in X10media x10 Automatic Mp3 Search Engine Script 1.5.5 through 1.6 allows remote attackers to read arbitrary files via an encoded url parameter, as demonstrated by obtaining database credentials from includes/constants.php.	2009-08-12	5.0	CVE-2008-6960 XF VUPEN BID MILWORM SECUNIA OSVDB
xmlsoft -- libxml xmlsoft -- libxml2	Stack consumption vulnerability in libxml2 2.5.10, 2.6.16, 2.6.26, 2.6.27, and 2.6.32, and libxml 1.8.17, allows context-dependent attackers to cause a denial of service (application crash) via a large depth of element declarations in a DTD, related to a function recursion, as demonstrated by the Codenomicon XML fuzzing framework.	2009-08-11	4.3	CVE-2009-2414 DEBIAN
xmlsoft -- libxml xmlsoft -- libxml2	Multiple use-after-free vulnerabilities in libxml2 2.5.10, 2.6.16, 2.6.26, 2.6.27, and 2.6.32, and libxml 1.8.17, allow context-dependent attackers to cause a denial of service (application crash) via crafted (1) Notation or (2) Enumeration attribute types in an XML file, as demonstrated by the Codenomicon XML fuzzing framework.	2009-08-11	4.3	CVE-2009-2416 DEBIAN
zeeways -- zeejobsite	Unrestricted file upload vulnerability in editresume_next.php in Zeeways ZEEJOBSITE 2.0 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension as a photo in a profile edit action, then accessing the file via a direct request to jobseekers/logos/.	2009-08-07	6.5	CVE-2008-6913 XF VUPEN BID MILWORM
zenphoto -- zenphoto	Cross-site scripting (XSS) vulnerability in function.php in Zenphoto 1.1.7 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors in the "request logging" feature. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-08-10	4.3	CVE-2008-6925 XF BID
zope -- zodb	Unspecified vulnerability in Zope Object Database (ZODB) before 3.8.2, when certain Zope Enterprise Objects (ZEO) database sharing is enabled, allows remote attackers to execute arbitrary Python code via vectors involving the ZEO network protocol.	2009-08-07	6.5	CVE-2009-0668 XF VUPEN BID SECUNIA SECUNIA CONFIRM OSVDB MLIST

[Back to top](#)

<b>Low Vulnerabilities</b>				
<b>Primary Vendor -- Product</b>	<b>Description</b>	<b>Published</b>	<b>CVSS Score</b>	<b>Source &amp; Patch Info</b>
ibm -- websphere_application_server	The Web Services functionality in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.25 and 7.0 before 7.0.0.5, in certain circumstances involving the ibm-webservicesclient-bind.xmi file and custom password encryption, uses weak password obfuscation, which allows local users to cause a denial of service (deployment failure) via unspecified vectors.	2009-08-13	2.1	<a href="#">CVE-2009-2087 CONFIRM CONFIRM</a>
ibm -- websphere_application_server	The Migration component in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.25 and 7.0 before 7.0.0.5, when tracing is enabled and a 6.1 to 7.0 migration has occurred, allows remote authenticated users to obtain sensitive information by reading a Migration Trace file.	2009-08-13	2.1	<a href="#">CVE-2009-2089 CONFIRM CONFIRM</a>
ibm -- websphere_commerce	Unspecified vulnerability in IBM WebSphere Commerce 6.0 Enterprise before 6.0.0.8, when trace is enabled, allows local users to obtain sensitive information via unknown vectors.	2009-08-13	1.5	<a href="#">CVE-2009-2094 CONFIRM</a>
karen_stevenson -- cck yves_chedemois -- cck	Multiple cross-site scripting (XSS) vulnerabilities in Drupal Content Construction Kit (CCK) 5.x through 5.x-1.8 allow remote authenticated users with "administer content" permissions to inject arbitrary web script or HTML via the (1) "field label," (2) "help text," or (3) "allowed values" settings.	2009-08-13	3.5	<a href="#">CVE-2008-6972 CONFIRM</a>
sun -- java_system_access_manager sun -- java_system_web_server sun -- opensso_enterprise	Sun Java System Access Manager 6.3 2005Q1, 7.0 2005Q4, and 7.1; and OpenSSO Enterprise 8.0; when AMConfig.properties enables the debug flag, allows local users to discover cleartext passwords by reading debug files.	2009-08-07	2.1	<a href="#">CVE-2009-2712 SUNALERT CONFIRM</a>

[Back to top](#)

Last updated August 17, 2009

 [Print This Document](#)